

COVER SHEET

Hewlett-Packard Docket Number:

10017334-1

Title:

Node, Method and Computer Readable Medium for Optimizing
Performance of Signature Rule Matching in a Network

Inventor(s):

Richard Paul Tarquini
110 Pahlmeyer Place
Apex, NC 27502

Richard Louis Schertz
117 Prynwood Ct.
Raleigh, NC 27607

5 NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING
PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK

10 TECHNICAL FIELD OF THE INVENTION

This invention relates to network technologies and, more particularly, to a node, method, and computer readable medium for optimizing performance of signature rule matching in a network.

15 CROSS-REFERENCE TO RELATED APPLICATIONS

This patent application is related to co-pending U.S. Patent Application, Serial No. _____, entitled "METHOD AND COMPUTER READABLE MEDIUM FOR SUPPRESSING EXECUTION OF SIGNATURE FILE DIRECTIVES DURING A NETWORK EXPLOIT," filed October 31, 2001, co-assigned herewith; U.S. Patent

20 Application, Serial No. _____, entitled "SYSTEM AND METHOD OF DEFINING THE SECURITY CONDITION OF A COMPUTER SYSTEM," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "SYSTEM AND METHOD OF DEFINING THE SECURITY VULNERABILITIES OF A COMPUTER SYSTEM," filed October 31,

25 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "SYSTEM AND METHOD OF DEFINING UNAUTHORIZED INTRUSIONS ON A COMPUTER SYSTEM," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "NETWORK

30 INTRUSION DETECTION SYSTEM AND METHOD," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "NODE, METHOD AND COMPUTER READABLE MEDIUM FOR INSERTING AN INTRUSION PREVENTION SYSTEM INTO A NETWORK STACK," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "METHOD, COMPUTER-READABLE MEDIUM, AND

- NODE FOR DETECTING EXPLOITS BASED ON AN INBOUND SIGNATURE OF THE EXPLOIT AND AN OUTBOUND SIGNATURE IN RESPONSE THERETO," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "NETWORK, METHOD AND COMPUTER
- 5 READABLE MEDIUM FOR DISTRIBUTED SECURITY UPDATES TO SELECT NODES ON A NETWORK," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "METHOD, COMPUTER READABLE MEDIUM, AND NODE FOR A THREE-LAYERED INTRUSION PREVENTION SYSTEM FOR DETECTING NETWORK EXPLOITS," filed
- 10 October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "SYSTEM AND METHOD OF AN OS-INTEGRATED INTRUSION DETECTION AND ANTI-VIRUS SYSTEM," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "METHOD, NODE AND COMPUTER READABLE MEDIUM FOR
- 15 IDENTIFYING DATA IN A NETWORK EXPLOIT," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "METHOD, NODE AND COMPUTER READABLE MEDIUM FOR PERFORMING MULTIPLE SIGNATURE MATCHING IN AN INTRUSION PREVENTION SYSTEM," filed October 31, 2001, co-assigned herewith; U.S. Patent
- 20 Application, Serial No. _____, entitled "USER INTERFACE FOR PRESENTING DATA FOR AN INTRUSION PROTECTION SYSTEM," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "NODE AND MOBILE DEVICE FOR A MOBILE TELECOMMUNICATIONS NETWORK PROVIDING INTRUSION
- 25 DETECTION," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "METHOD AND COMPUTER-READABLE MEDIUM FOR INTEGRATING A DECODE ENGINE WITH AN INTRUSION DETECTION SYSTEM," filed October 31, 2001, co-assigned herewith; U.S. Patent Application, Serial No. _____, entitled "SYSTEM AND
- 30 METHOD OF GRAPHICALLY DISPLAYING DATA FOR AN INTRUSION PROTECTION SYSTEM," filed October 31, 2001, co-assigned herewith; and U.S.

TOP SECRET - DRAFT - 2000

Patent Application, Serial No. _____, entitled "SYSTEM AND METHOD OF GRAPHICALLY CORRELATING DATA FOR AN INTRUSION PROTECTION SYSTEM," filed October 31, 2001, co-assigned herewith.

5 **BACKGROUND OF THE INVENTION**

Network-exploit attack tools, such as denial-of-service (DoS) attack utilities, are becoming increasing sophisticated and, due to evolving technologies, simple to execute. Relatively unsophisticated attackers can arrange, or be involved in, computer system compromises directed at one or more targeted facilities. A network system 10 attack (also referred to herein as an intrusion) is an unauthorized or malicious use of a computer or computer network and may involve hundred or thousands of unprotected, or alternatively compromised, Internet nodes together in a coordinated attack on one or more selected targets.

Network attack tools based on the client/server model have become a preferred 15 mechanism for executing network attacks on targeted networks or devices. High capacity machines in networks having deficient security are often desired by attackers to launch distributed attacks therefrom. University servers typically feature high connectivity and capacity but relatively mediocre security. Such networks also often have inexperienced or overworked network administrators making them even more 20 vulnerable for involvement in network attacks.

Network-exploit attack tools, comprising hostile attack applications such as denial-of-service utilities, responsible for transmitting data across a network medium will often have a distinctive "signature," or recognizable pattern within the transmitted data. The signature may comprise a recognizable sequence of particular packets 25 and/or recognizable data that is contained within one or more packets. Signature analysis is often performed by a network intrusion prevention system (IPS) and may be implemented as a pattern-matching algorithm and may comprise other signature recognition capabilities as well as higher-level application monitoring utilities. A simple signature analysis algorithm may search for a particular string that has been 30 identified as associated with a hostile application. Once the string is identified within a network data stream, the one or more packets carrying the string may be identified as

10017334-1

"hostile," or exploitative, and the IPS may then perform any one or more of a number of actions, such as logging the identification of the frame, performing a countermeasure, or performing another data archiving or protection measure.

Intrusion prevention systems (IPS) encompass technology that attempts to
5 identify exploits against a computer system or network of computer systems. Numerous types of IPSs exist and each are generally classified as either a network-based, host-based, or node-based IPS.

Network-based IPS appliances are typically dedicated systems placed at strategic places on a network to examine data packets to determine if they coincide
10 with known attack signatures. To compare packets with known attack signatures, network-based IPS appliances utilize a mechanism referred to as passive protocol analysis to inconspicuously monitor, or "sniff," all traffic on a network and to detect low-level events that may be discerned from raw network traffic. Network exploits may be detected by identifying patterns or other observable characteristics of network
15 frames. Network-based IPS appliances examine the contents of data packets by parsing network frames and packets and analyzing individual packets based on the protocols used on the network. A network-based IPS appliance inconspicuously monitors network traffic inconspicuously, i.e., other network nodes may be, and often are, unaware of the presence of the network-based IPS appliance. Passive monitoring
20 is normally performed by a network-based IPS appliance by implementation of a "promiscuous mode" access of a network interface device. A network interface device operating in promiscuous mode copies packets directly from the network media, such as a coaxial cable, 100baseT or other transmission medium, regardless of the destination node to which the packet is addressed. Accordingly, there is no simple
25 method for transmitting data across the network transmission medium without the network-based IPS appliance examining it and thus the network-based IPS appliance may capture and analyze all network traffic to which it is exposed. Upon identification of a suspicious packet, i.e., a packet that has attributes corresponding to a known attack signature monitored for occurrence by the network-based IPS
30 appliance, an alert may be generated thereby and transmitted to a management module of the IPS so that a networking expert may implement security measures. Network-

based IPS appliances have the additional advantage of operating in real-time and thus can detect an attack as it is occurring. Moreover, a network-based IPS appliance is ideal for implementation of a state-based IPS security measure that requires accumulation and storage of identified suspicious packets of attacks that may not be
5 identified “atomically,” that is by a single network packet. For example, transmission control protocol (TCP) synchronization (SYN) flood attacks are not identifiable by a single TCP SYN packet but rather are generally identified by accumulating a count of TCP SYN packets that exceed a predefined threshold over a defined period of time. A network-based IPS appliance is therefore an ideal platform for implementing state-
10 based signature detection because the network-based IPS appliance may collect all such TCP SYN packets that pass over the local network media and thus may properly archive and analyze the frequency of such events.

However, network-based IPS appliances may often generate a large number of “false positives,” i.e., incorrect diagnoses of an attack. False positive diagnoses by
15 network-based IPS appliances result, in part, due to errors generated during passive analysis of all the network traffic captured by the IPS that may be encrypted and formatted in any number of network supported protocols. Content scanning by a network-based IPS is not possible on an encrypted link although signature analysis based on protocol headers may be performed regardless of whether the link is
20 encrypted or not. Additionally, network-based IPS appliances are often ineffective in high speed networks. As high speed networks become more commonplace, software-based network-based IPS appliances that attempt to sniff all packets on a link will become less reliable. Most critically, network-based IPS appliances can not prevent attacks unless integrated with, and operated in conjunction with, a firewall protection
25 system.

Host-based IPSs detect intrusions by monitoring application layer data. Host-based IPSs employ intelligent agents to continuously review computer audit logs for suspicious activity and compare each change in the logs to a library of attack signatures or user profiles. Host-based IPSs may also poll key system files and
30 executable files for unexpected changes. Host-based IPSs are referred to as such because the IPS utilities reside on the system to which they are assigned to protect.

Host-based IPSs typically employ application-level monitoring techniques that examine application logs maintained by various applications. For example, a host-based IPS may monitor a database engine that logs failed access attempts and/or modifications to system configurations. Alerts may be provided to a management node upon identification of events read from the database log that have been identified as suspicious. Host-based IPSs, in general, generate very few false-positives. However, host-based IPS such as log-watchers are generally limited to identifying intrusions that have already taken place and are also limited to events occurring on the single host. Because log-watchers rely on monitoring of application logs, any damage resulting from the logged attack will generally have taken place by the time the attack has been identified by the IPS. Some host-based IPSs may perform intrusion-preventative functions such as ‘hooking’ or ‘intercepting’ operating system application programming interfaces to facilitate execution of preventative operations by an IPS based on application layer activity that appears to be intrusion-related.

Because an intrusion detected in this manner has already bypassed any lower level IPS, a host-based IPS represents a last layer of defense against network exploits. However, host-based IPSs are of little use for detecting low-level network events such as protocol events.

Node-based IPSs apply the intrusion detection and/or prevention technology on the system being protected. An example of node-based IPS technologies is inline intrusion detection. A node-based IPS may be implemented at each node of the network that is desired to be protected. Inline IPSs comprise intrusion detection technologies embedded in the protocol stack of the protected network node. Because the inline IPS is embedded within the protocol stack, both inbound and outbound data will pass through, and be subject to monitoring by, the inline IPS. An inline IPS overcomes many of the inherent weaknesses of network-based solutions. As mentioned hereinabove, network-based solutions are generally ineffective when monitoring high-speed networks due to the fact that network-based solutions attempt to monitor all network traffic on a given link. Inline intrusion prevention systems, however, only monitor traffic directed to the node on which the inline IPS is installed. Thus, attack packets can not physically bypass an inline IPS on a targeted machine

because the packet must pass through the protocol stack of the targeted device. Any bypassing of an inline IPS by an attack packet must be done entirely by ‘logically’ bypassing the IPS, i.e., an attack packet that evades an inline IPS must do so in a manner that causes the inline IPS to fail to identify, or improperly identify, the attack 5 packet. Additionally, inline IPSs provide the hosting node with low-level monitoring and detection capabilities similar to that of a network IPS and may provide protocol analysis and signature matching or other low-level monitoring or filtering of host traffic. The most significant advantage offered by inline IPS technologies is that attacks are detected as they occur. Whereas host-based IPSs determine attacks by 10 monitoring system logs, inline intrusion detection involves monitoring network traffic and isolating those packets that are determined to be part of an attack against the hosting server and thus enabling the inline IPS to actually prevent the attack from succeeding. When a packet is determined to be part of an attack, the inline IPS layer may discard the packet thus preventing the packet from reaching the upper layer of the 15 protocol stack where damage may be caused by the attack packet - an effect that essentially creates a local firewall for the server hosting the inline IPS and protecting it from threats coming either from an external network, such as the Internet, or from within the network. Furthermore, the inline IPS layer may be embedded within the protocol stack at a layer where packets have been unencrypted so that the inline IPS is 20 effective operating on a network with encrypted links. Additionally, inline IPSs can monitor outgoing traffic because both inbound and outbound traffic respectively destined to and originating from a server hosting the inline IPS must pass through the protocol stack.

Although the advantages of inline IPS technologies are numerous, there are 25 drawbacks to implementing such a system. Inline intrusion detection is generally processor intensive and may adversely effect the node’s performance hosting the detection utility. Additionally, inline IPSs may generate numerous false positive attack diagnoses. Furthermore, inline IPSs cannot detect systematic probing of a network, such as performed by reconnaissance attack utilities, because only traffic at 30 the local server hosting the inline IPS is monitored thereby.

Each of network-based, host-based and inline-based IPS technologies have respective advantages as described above. Ideally, an intrusion prevention system will incorporate all of the aforementioned intrusion detection strategies. Additionally, an IPS may comprise one or more event generation mechanisms that report identifiable events to one or more management facilities. An event may comprise an identifiable series of system or network conditions or it may comprise a single identified condition. An IPS may also comprise an analysis mechanism or module and may analyze events generated by the one or more event generation mechanisms. A storage module may be comprised within an IPS for storing data associated with intrusion-related events. A countermeasure mechanism may also be comprised within the IPS for executing an action intended to thwart, or negate, a detected exploit.

IPS signature processing may be performed “inline” or “offline.” Frames are parsed and analyzed against known attack signatures as the frames are received by the network and/or node during inline processing. Because the signature analysis is executed in real time, that is as the frames are received, performance is critical because positive identifications may require proactive actions on the part of the IPS, such as signaling a management node, archiving of the subject frame, discarding of the subject frame, or performing another countermeasure. IPS systems that operate offline do not perform signature analysis of network frames in real-time. Rather, network frames are captured into a memory device and the recorded traffic is scanned for signature analysis at a later time. However, offline IPSs may benefit from performance optimization techniques that are implemented on inline based IPSs as well.

25 **SUMMARY OF THE INVENTION**

In accordance with an embodiment of the present invention, a node of a network for managing an intrusion protection system, the node comprising a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit and an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management

application operable to receive text-file input from an input device, the text-file defining a network-exploit rule and comprising at least one field is provided.

In accordance with another embodiment of the present invention, a method of distributing command and security updates in a network having an intrusion protection system comprising generating a text-file defining a network-exploit rule and specifying at least one field selected from the group consisting of an ENABLED field value and a SEVERITY level field value during generation of the text-file is provided.

In accordance with yet another embodiment of the present invention, a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of reading input from an input device of the computer, compiling the input into a machine-readable signature file comprising machine-readable logic representative of the network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field, evaluating the machine-readable signature file, and determining the value of the at least one field of the machine-readable signature file is provided.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, the objects and advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

FIGURE 1 illustrates an exemplary arrangement for executing a computer system compromise according to the prior art;

FIGURE 2 illustrates a comprehensive intrusion prevention system employing network-based and hybrid host-based and node based intrusion detection technologies according to an embodiment of the invention;

FIGURE 3 is an exemplary network protocol stack according to the prior art;

FIGURE 4 illustrates a network node that may run an instance of an intrusion protection system application according to an embodiment of the present invention; and

FIGURE 5 illustrates an exemplary network node that may operate as a management node within a network protected by the intrusion protection system according to an embodiment of the present invention.

5 **DETAILED DESCRIPTION OF THE DRAWINGS**

The preferred embodiment of the present invention and its advantages are best understood by referring to FIGURES 1 through 5 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

In FIGURE 1, there is illustrated an exemplary arrangement for executing a computer system compromise - the illustrated example showing a simplified distributed intrusion network 40 arrangement typical of distributed system attacks directed at a target machine 30. An attack machine 10 may direct execution of a distributed attack by any number of attack agents 20A-20N by one of numerous techniques such as remote control by IRC "robot" applications. Attack agents 20A-20N, also referred to as "zombies" and "attack agents," are generally computers that are available for public use or that have been compromised such that a distributed attack may be launched upon command of an attack machine 10. Numerous types of distributed attacks may be launched against a target machine 30. The target machine 30 may suffer extensive damage from simultaneous attack by attack agents 20A-20N and the attack agents 20A-20N may be damaged from the client attack application as well. A distributed intrusion network may comprise an additional layer of machines involved in an attack intermediate the attack machine 10 and attack agents 20A-20N. These intermediate machines are commonly referred to as "handlers" and each handler may control one or more attack agents 20A-20N. The arrangement shown for executing a computer system compromise is illustrative only and may compromise numerous arrangements that are as simple as a single attack machine 10 attacking a target machine 30 by, for example, sending malicious probe packets or other data intended to compromise target machine 30. Target machine may be, and often is, connected to a larger network and access thereto by attack machine 10 may cause damage to a large collection of computer systems commonly located within the network.

- In FIGURE 2, there is illustrated a comprehensive intrusion prevention system employing network-based and hybrid host-based/node-based intrusion detection technologies according to an embodiment of the invention. One or more networks 100 may interface with the Internet 50 via a router 45 or other device. In the 5 illustrative example, two Ethernet networks 55 and 56 are comprised in network 100. Ethernet network 55 comprises a web-content server 270A and a file transport protocol- content server 270B. Ethernet network 56 comprises a domain name server 270C, a mail server 270D, a database sever 270E and a file server 270F. A firewall/proxy router 60 disposed intermediate Ethernets 55 and 56 provides security 10 and address resolution to the various systems of network 56. A network-based IPS appliance 80 and 81 is respectively implemented on both sides of firewall/proxy router 60 to facilitate monitoring of attempted attacks against one or more elements of Ethernets 55 and 56 and to facilitate recording successful attacks that successfully penetrate firewall/proxy router 60. Network-based IPS appliances 80 and 81 may 15 respectively comprise (or alternatively be connected to) a database 80A and 81A of known attack signatures, or rules, against which network frames captured thereby may be compared. Alternatively, a single database (not shown) may be centrally located within network 100 and may be accessed by network-based IPS appliances 80 and 81. Accordingly, network-based IPS appliance 80 may monitor all packets inbound from 20 Internet 50 to network 100 arriving at Ethernet network 55. Similarly, a network-based IPS appliance 81 may monitor and compare all packets passed by firewall/proxy router 60 for delivery to Ethernet network 56. An IPS management node 85 may also be part of network 100 to facilitate configuration and management of the IPS components in network 100.
- 25 In view of the above-noted deficiencies of network-based intrusion prevention systems, a hybrid host-based and node-based intrusion prevention system is preferably implemented within each of the various nodes, such as servers 270A-270N (also referred to herein as "nodes"), of Ethernet networks 55 and 56 in the secured network 100. Management node 85 may receive alerts from respective nodes within network 30 100 upon detection of an intrusion event by any one of the network-based IPS appliances 80 and 81 as well as any of the nodes of network 100 having a hybrid

agent-based and node-based IPS implemented thereon. Additionally, each node 270A-270F may respectively employ a local file system for archiving intrusion-related events, generating intrusion-related reports, and storing signature files against which local network frames and/or packets are examined.

- 5 Preferably, network-based IPS appliances 80 and 81 are dedicated entities for monitoring network traffic on associated Ethernets 55 and 56 of network 100. To facilitate intrusion detection in high speed networks, network-based IPS appliances 80 and 81 preferably comprise a large capture RAM for capturing packets as they arrive on respective Ethernet networks 55 and 56. Additionally, it is preferable that
- 10 network-based IPS appliances 80 and 81 respectively comprise hardware-based filters for filtering network traffic, although IPS filtering by network-based IPS appliances 80 and 81 may be implemented in software. Moreover, network-based IPS appliances 80 and 81 may be configured, for example by demand of IPS management node 85, to monitor one or more specific devices rather than all devices on a common network.
- 15 For example, network-based IPS appliance 80 may be directed to monitor only network data traffic addressed to web server 270A.

Hybrid host-based/node-based intrusion prevention system technologies may be implemented on all nodes 270A-270N on Ethernet networks 55 and 56 that may be targeted by a network attack. In general, each node is comprised of a reprogrammable computer having a central processing unit (CPU), a memory module operable to store machine-readable code that is retrievable and executable by the CPU, and may further comprise various peripheral devices, such as a display monitor, a keyboard, a mouse or another device, connected thereto. A storage media, such as a magnetic disc, an optical disc or another component operable to store data, may be connected to 20 memory module and accessible thereby and may provide one or more databases for archiving local intrusion events and intrusion event reports. An operating system may be loaded into memory module, for example upon bootup of the respective node, and comprises an instance of a protocol stack as well as various low-level software modules required for tasks such as interfacing to peripheral hardware, scheduling of 25 tasks, allocation of storage as well as other system tasks. Each node protected by the hybrid host-based and node-based IPS of the present invention accordingly has an IPS

software application maintained within the node, such as in a magnetic hard disc, that is retrievable by the operating system and executable by the central processing unit. Additionally, each node executing an instance of the IPS application has a local database from which signature descriptions of documented attacks may be fetched
5 from storage and compared with a packet or frame of data to detect a correspondence therebetween. Detection of a correspondence between a packet or frame at an IDS server may result in execution of any one or more of various security procedures.

The IPS described with reference to FIGURE 2 may be implemented on any number of platforms. Each hybrid host-based/node-based instance of the IPS application described herein is preferably implemented on a network node, such as web server 270A operated under control of an operating system, such as Windows NT 4.0 that is stored in a main memory and running on a central processing unit, and attempts to detect attacks targeted at the hosting node. The particular network 100 illustrated in FIGURE 2 is exemplary only and may comprise any number of network servers. Corporate, and other large scale, networks may typically comprise numerous individual systems providing similar services. For example, a corporate network may comprise hundreds of individual web servers, mail servers, FTP servers and other systems providing common data services.
10
15

Each operating system of a node incorporating an instance of an IPS application additionally comprises a network protocol stack 90, as illustrated in FIGURE 3, that defines the entry point for frames received by a targeted node from the network, e.g. the Internet or Intranet. Network stack 90 as illustrated is representative of the well-known WindowsNT (TM) system network protocol stack and is so chosen to facilitate discussion and understanding of the invention. However,
20 it should be understood that the invention is not limited to a specific implementation of the illustrated network stack 90 but, rather, stack 90 is described to facilitate understanding of the invention. Network stack 90 comprises a transport driver interface (TDI) 125, a transport driver 130, a protocol driver 135 and a media access control (MAC) driver 145 that interfaces with the physical media 101. Transport
25 driver interface 125 functions to interface the transport driver 130 with higher-level file system drivers. Accordingly, TDI 125 enables operating system drivers, such as
30

- network redirectors, to activate a session, or bind, with the appropriate protocol driver 135. Accordingly, a redirector can access the appropriate protocol, for example UDP, TCP, NetBEUI or other network or transport layer protocol, thereby making the redirector protocol-independent. The protocol driver 135 creates data packets that are
5 sent from the computer hosting the network protocol stack 90 to another computer or device on the network or another network via the physical media 101. Typical protocols supported by an NT network protocol stack comprise NetBEUI, TCP/IP, NWLink, Data Link Control (DLC) and AppleTalk although other transport and/or network protocols may be comprised. MAC driver 145, for example an Ethernet
10 driver, a token ring driver or other networking driver, provides appropriate formatting and interfacing with the physical media 101 such as a coaxial cable or another transmission medium.

15 The capabilities of the host-based IPS comprise application monitoring of: file system events; registry access; successful security events; failed security events and suspicious process monitoring. Network access applications, such as Microsoft IIS and SQL Server, may also have processes related thereto monitored.

20 Intrusions may be prevented on a particular IPS host by implementation of inline, node-based monitoring technologies. The inline-IPS is preferably comprised as part of a hybrid host-based/node-based IPS although it may be implemented independently of any host-based IPS system. The inline-IPS will analyze packets received at the hosting node and perform signature analysis thereof against a database of known signatures by network layer filtering.

25 In FIGURE 4, there is illustrated a network node 270 that may run an instance of an IPS application 91 and thus operate as an IPS server. IPS application 91 may be implemented as a three-layered IPS, as described in co-pending application entitled “Method and Computer Readable Medium for a Three-Layered Intrusion Prevention System for Detecting Network Exploits” and filed concurrently herewith, and may comprise a server application and/or a client application. Network node 270, in general, comprises a central processing unit (CPU) 272 and a memory module 274
30 operable to store machine-readable code that is retrievable and executable by CPU 272 via a bus (not shown). A storage media 276, such as a magnetic disc, an optical

disc or another component operable to store data, may be connected to memory module 274 and accessible thereby by the bus as well. An operating system 275 may be loaded into memory module 274, for example upon bootup of node 270, and comprises an instance of protocol stack 90 and may have an intrusion prevention system application 91 loaded from storage media 276. One or more network exploit rules, an exemplary form described in co-pending application entitled "Method, Node and Computer Readable Medium for Identifying Data in a Network Exploit" and filed concurrently herewith, may be compiled into a machine-readable signature(s) and stored within a database 277 that is loadable into memory module 274 and may be retrieved by IPS application 91 for facilitating analysis of network frames and/or packets.

In FIGURE 5, there is illustrated an exemplary network node that may operate as a management node 85 of the IPS of a network 100. Management node 85, in general, comprises a CPU 272 and a memory module 274 operable to store machine-readable code that is retrievable and executable by CPU 272 via a bus (not shown). A storage media 276, such as a magnetic disc, an optical disc or another component operable to store data, may be connected to memory module 274 and accessible thereby by the bus as well. An operating system 275 may be loaded into memory module 274, for example upon bootup of node 85, and comprises an instance of protocol stack 90. Operating system 275 is operable to fetch an IPS management application 279 from storage media 276 and load management application 279 into memory module 274 where it may be executed by CPU 272. Node 85 preferably has an input device 281, such as a keyboard, and an output device 282, such as a monitor, connected thereto.

An operator of management node 85 may input one or more text-files 277A-277N via input device 281. Each text-file 277A-277N may define a network-based exploit and comprise a logical description of an attack signature as well as IPS directives to execute upon an IPS evaluation of an intrusion-related event associated with the described attack signature. Each text file 277A-277N may be stored in a database 278A on storage media 276 and compiled by a compiler 280 into a respective machine-readable signature file 281A-281N that is stored in a database 278B. Each of

T01201702820001

the machine-readable signature files 281A-281N comprises binary logic representative of the attack signature as described in the respectively associated text-file 277A-277N. An operator of management node 85 may periodically direct management node 85, through interaction with a client application of IPS application 279 via input device

- 5 281, to transmit one or more machine-readable signature files (also generally referred to herein as "signature files") stored in database 278B to a node, or a plurality of nodes, in network 100. Alternatively, signature files 281A-281N may be stored on a computer-readable medium, such as a compact disk, magnetic floppy disk or another portable storage device, and installed on node 270 of network 100. Application 279 is
- 10 preferably operable to transmit all such signature-files 281A-281N, or one or more subsets thereof, to a node, or a plurality of nodes, in network 100. Preferably, IPS application 279 provides a graphical user interface on output device 282 for facilitating input of commands thereto by an operator of node 85.

Optimization techniques for performance enhancement and reduction of memory requirements are particularly desirable when implemented in an IPS application that may perform real-time, processor-intensive network filtering. The present invention provides optimization techniques that allow restricting the number of signatures that a network IPS application and/or a network node-based IPS appliance has to process. Preferably, such optimization techniques are made prior to initialization of a signature matching engine of an IPS application 91 and prior to modifications made to the set of signatures against which network traffic is compared.

As aforementioned, attack signatures may be defined in text-files and computer-readable signature files generated therefrom may be distributed throughout a network 100 and stored in a database 277 accessible by each node 270 of network 100 running an instance of IPS application 91. Database 277 storing one or more machine-readable signature files may be fed to an instance of IPS application 91 executed by CPU 272 and network frame analysis may be performed by an associative process engine of IPS 91. IPS application 91 may then inspect inbound and/or outbound network traffic against one or more signature files maintained in database 277. Each signature file maintained in database 277 is preferably generated from compilation of a text-file and may also define one or more actions, or directives, to be

performed upon identification of a correspondence between a signature of an analyzed packet and a respective machine-readable signature-file. For example, a text-file defining a network exploit may specify a particular security measure, such as specifying that the identified packet is to be discarded, reported to management node 85, archived, or that another security measure is to be executed, and the corresponding machine-readable signature-file generated therefrom may comprise machine-readable instructions directing IPS application 91 to perform the specified security measure.

Preferably, text-file 277A comprised of a text-based network exploit rule defines an exploit-signature and allows an operator or other network 100 personnel

- 10 operating management node 85 to set a security policy associated with a particular signature by specifying a security policy in text-file 277A. A basic optimization may comprise simply enabling or disabling enforcement of intrusion prevention of the signature defined in text-file 277A by specifying a value in an enable/disable field of text-file 277A, such as specifying a boolean value or an otherwise asserted or de-asserted value thereto. Additional optimizations may allow various levels of specified priority levels to be assigned to each of the defined network exploit rules in a priority, or severity, field. Implementation of signature matching may then be restricted to a specific priority level and/or to any signatures meeting or exceeding a particular priority level. Thus, the enable/disable field of a network exploit rule defined in text-
20 file 277A, as well as the priority level field, may be used to generate a subset of all signature descriptions to be distributed throughout network 100 protected by the IPS. Accordingly, the number of network exploit rules scanned by IPS application 91 may be periodically varied by, for example, a network manager operating management node 85.

25 Additional filtering may be performed to further enhance signature analysis of network frames performed by a network-based, node-based, and/or a host-based IPS server. For example, a particular node (comprising a network-based IPS appliance) may be configured to only filter network traffic on a particular set of protocols. Signatures maintained in database 277 and generated from text-file 277A defining a
30 protocol-specific attack not comprised within the particular set of protocols may then be ignored or discarded by IPS 91. Similarly, all network nodes may comprise default

protocols that are not filtered if, for example, network 100 does not allow data transmissions in the particular protocol. Accordingly, signature descriptions of attacks made in a protocol that is inapplicable to network 100 transmissions may be discarded, or otherwise ignored, by all instances of IPS 91 running on nodes within network 100. Other optimization techniques are possible as described with reference to co-pending application [10002019].

In TABLE A, there is an exemplary portion of a text-based attack signature description that may be defined in text-file 277A and that comprises enablement and priority attributes therein from which compilation thereof by compiler 280 may generate a machine-readable signature-file and associated enablement and priority attribute logic. The particular portion of the signature description shown describes an attack known as 'Ping of Death.'

TABLE A

```
BEGIN_SECURITY_DEF: PingofDeath
PLATFORM:ALL
ENABLED:1
BRIEF_DESCRIPTION: 'DETECT PING OF DEATH'
EXPLANATION: 'The Ping of Death attack exploits a flaw in the TCP/IP stack implementation in
which the TCP/IP stack does not validate the total length of the IP frame.'
SEVERITY:2
```

As shown, an ENABLED field is comprised in the text-based description that
15 may be comprised in text-file 277A. In the present example, the ENABLED field has
an asserted value of 1 indicating that intrusion protection from an attack having a
signature corresponding to the machine-readable signature-file generated from the
described text-file is to be enabled by IPS application 91. The ENABLED field may
alternatively be de-asserted, for example assigned a value of 0, to disable protection
20 by any node of network 100 running IPS application 91 and receiving a machine-
readable signature-file generated from associated text-file 277A.

Additionally, the text-based signature description may further comprise a
priority, or SEVERITY, field that may have a numerical value assigned thereto and
that specifies a priority value for intrusion protection from an attack having a
signature that corresponds to a machine-readable signature-file generated from
25

compilation of the text-file. The exemplary attack signature has a SEVERITY field value of 2 assigned thereto. Thus, a threshold may be supplied to IPS application 91 and any machine-readable signature files generated from respective text-files 277A-277N having a SEVERITY less than the specified threshold may be ignored by IPS 5 application 91. Accordingly, only machine-readable signatures having SEVERITY values equal to or greater than a specified threshold are retrieved from database 277 and utilized for signature analysis of network frames by IPS application 91.

With reference again to FIGURE 5, management node 85 of an IPS comprises CPU 272 and memory module 274. Storage media 276, such as a magnetic disc, an 10 optical disc or another component operable to store data, may be connected to memory module 274 and accessible thereby. Operating system 275 may be loaded into memory module 274, for example upon bootup of node 85, and comprises an instance of protocol stack 90. Operating system 275 is operable to fetch an IPS management application 279 from storage media 276 and load management 15 application 279 into memory module 274 where it may be executed by CPU 272. Node 85 preferably has an input device 281, such as a keyboard, and an output device 282, such as a monitor, connected thereto. An operator of management node 85 may input one or more text-files 277A-277N via input device 281 and each text-file may, in addition to comprising a text-based signature description or rule, comprise an 20 ENABLED field and a SEVERITY field. As described, the ENABLED field may have a boolean value assigned thereto during input of the text-file. A value may be assigned, via input device 281, during input of the text-file to the SEVERITY field as well. An operator of management node 85 may periodically direct management node 85, through interaction with application 279 via input device 281, to compile one or 25 more text-files 270A-270N into respectively associated machine-readable signature files 281A-281N that may be stored in database 278B. Each machine-readable signature-file may comprise, in addition to binary signature data, machine-readable logic representative of the ENABLED and/or SEVERITY field values. Management node 85 may additionally engage in communications with one or more nodes of 30 network 100, for example by a TCP session managed by network stack 90 of the operating system 275, and transmit one or more machine-readable signature-files

101307-1026383001

stored in database 278B to a node 270, or a plurality of nodes, in network 100.

Application 279 is preferably operable to transmit all machine-readable signature-files, or one or more subsets thereof, to a node 270, or a plurality of nodes, in network 100. Preferably, application 279 provides a graphical user interface on output device

- 5 282 for facilitating input of commands thereto by an operator of management node 85. Accordingly, transmission of one or more subsets of machine-readable signature-files may be contingent on supply of a transmission directive specifying transmission of only machine-readable signature-files generated from compilation of a text-file having an ENABLED field value asserted and/or a SEVERITY field having a value equal to
10 or greater than a threshold specified in the transmission directive. Accordingly, only machine-readable signature-files generated from text-files having an ENABLED and/or a SEVERITY field satisfying an enablement and/or severity specification of a transmission directive supplied to management node 85 are transmitted to one or more nodes of network 100.

15 Alternatively, machine-readable signature-files may be distributed to one or more nodes of network 100 generated from text-files having an ENABLED and/or SEVERITY field and respective values assigned thereto. The machine-readable signature-files may be stored in database 277 and enablement and/or severity value specifications, or thresholds, may be supplied to IPS application 91. IPS application

20 91 may then retrieve only machine-readable signature-files from database 277 that have been generated from text-files having a ENABLED and/or SEVERITY field value that satisfies the enablement and/or severity value specifications supplied to IPS application 91. Supply of an enablement and/or a severity specification to IPS application 91 may be performed locally at the respective node running IPS

25 application 91, for example through a peripheral input device, or the enablement and/or severity specification may be supplied to the node remotely, for example via management node 85 engaging in a TCP session with the node.

Thus, the present invention provides a mechanism for optimizing the set of machine-readable signatures that are used in frame and packet analysis performed by

30 an IPS application by reducing the number of signature files that are checked by a processing engine of an IPS. Potential processing problems related to a large quantity

of machine-readable signature files that must be processed by an IPS are accordingly alleviated by the optimization technique of the present invention.

10003820-103101